文章
Qiao Peng · 四月 14, 2022 阅读大约需 11 分钟

InterSystems 数据平台与三级等保 - 第三篇

8. 应用安全

InterSystems数据平台上可能运行着多种应用，例如Web网页应用、SOAP服务、REST API、HL7 接口、SQL服务等等。这些应用种类繁多，面临的安全风险也是巨大的，例如代码注入攻击和HTTP的跨站请求伪造攻击等。

这其中代码注入攻击和针对Web应用的攻击尤其需要重视。

8.1 代码注入攻击

代码注入攻击通常和我们编写的程序相关，需要在程序编写时注意避免。

8.1.1 SQL注入攻击

SQL注入攻击是典型的代码注入攻击，通过从外部注入恶意SQL语句获得数据权限并获得敏感数据。关系型访问方式都是通过客户端SQL语句传入执行的，因此它是数据库重点需要防范的。

InterSystems数据平台并不支持以分号分割的多条SQL语句作为一个SQL命令执行，因此它本身免疫了主要的SQL注入攻击手段。

InterSystems数据平台支持***动态SQL***，即允许SQL命令作为方法的字符串参数传入，这会给SQL注入攻击留有隐患。在编程时，应避免开放服务用于接受完整的SQL语句作为参数，而是通过SQL动态传参来构建运行时SQL。

InterSystems数据平台支持行级安全，这有助于避免在SQL注入攻击时，将所有数据返回给攻击请求。

8.1.2 $ZF

InterSystems数据平台提供了系统函数$ZF，用以调用外部命令。其中$ZF(-1)和$ZF(-2)用以调用服务器操作系统的命令。这可能会成为代码攻击的隐患。

在使用$ZF开发服务时，应避免把完整的操作系统命令作为字符串参数传入来执行，而应仅传入

必要的数据，由服务器端方法来组成需要执行的操作系统命令，避免注入攻击。

8.2 Web应用安全管理

InterSystems数据平台提供多种Web应用，都是基于HTTP/HTTPS协议的，例如InterSystems数据平台的管理门户网页、用户自定义的网页、开放的SOAP服务、RESTful API。

既然走HTTP/HTTPS，所以首先应该部署专用Web服务器，并配置HTTPS来提供这些Web服务，在传输通道上保障安全。

除了传输通道，要得到更安全的生产环境，还有其它的安全设置需要检查和配置。

8.2.1 CSP/ZEN用户自定义网页应用

每个InterSystems数据平台等命名空间默认都有一个Web应用，可以通过它提供用户自定义网页应用。也可以创建一个新的Web应用提供用户自定义的网页应用。

第一个要检查的项目，是要看看这些默认创建的Web应用是否需要。如果不需要，应该禁用 – 取消选中“ Enable Application ”。

第二个要检查的项目，是这个Web应用使用的身份认证方式。在生产环境上，不应该使用“ 未验证 ”方式，所以应该取消选中该选项。

第三个要设置合适的“ 必要的资源 ”，它是对网页应用的资源权限要求。必须具有该资源的使用权限的用户，才能访问该网页应用。

第四个要决定是否开启防CSRF攻击，建议开启“ Prevent Login CSRF attack ”。

8.2.2管理门户

InterSystems
数据平台的管理门户就是CSP/ZEN开发的网页应用，它具有大部分系统管理和监控能力，例如安全配置、高可用配置等。

除了8.2.1提到的对网页应用的安全配置项目之外，InterSystems数据平台预置了一系列系统角色和系统资源，用于让不同用户对管理门户的不同功能页面具有不同的权限。例如操作员角色（%Operator）不具有创建、修改用户的权限。

这些用户权限检查是通过配置给管理页面的系统资源来判断的，只有对这些页面系统资源有权限的用户才能访问该管理页面。

为了提供更细颗粒度的管理，除了配置给管理门户页面上的系统资源，用户可以将自定义资源加到管理门户页面上。这样，用户需要同时具有系统定义的页面资源权限和用户自定义资源权限才能访问和使用管理页面。

如何
查看系统
预置的管理页面资
源和配置自定义资源？在每个管理门
户页面菜单项上，都有

链接，点击它就可以查看该管理页面分配的系统资源和自定义资源。如果要添加自定义资源，点击“ 分配 ”，就可以在弹出的页面中进行配置。

通过配置自定义资源，可以实现任意颗粒度的管理门户权限控制。

如果您在管理互操作产品，想了解系统提供的预定义安全资源，可以参考文档

8.2.3 SOAP服务

除了SQL服务，SOAP服务是InterSystems数据平台经常要开放的服务类型之一。如果您的生产环境上开放了SOAP服务，应该检查它的安全配置。

开启SOAP服务

InterSystems
数据平台的SOAP服务也是通过Web应用开放的。默认情况下，Web应用是没有开放“ 入站Web服务 ”的，也就是说默认Web应用是不能提供SOAP服务的。如果需要开放SOAP服务，需要选中对应Web应用的“ 入站Web服务 ”。

注意：如何仅是查看WSDL，并不需要开启此选项。

开启SOAP服务测试页功能

InterSystems
数据平台还提供SOAP服务测试页功能，该功能可以使用Web页面来测试SOAP服务，而不需要通过SOAPUI等工具。

为了安全，默认SOAP服务测试页功能是未开启的。如果需要开启，需要通过系统安全设置项开启：

```
SET ^SYS("Security","CSP","AllowPrefix",<SOAP????>,"%SOAP.")=1
```

注意：

1. <SOAP应用路径>最后需要加"/"，例如 "/csp/user/"

2. 该设置项不影响SOAP服务，仅影响测试页

SOAP认证与权限

在生产环境上，不应该发布无需认证的SOAP服务。因此也需要取消选中“ 未验证 ”方式。

同时通过“ 必要的资源 ”设置，可以为SOAP服务指定需要的权限。

SOAP安全协议

另外，SOAP本身有很多安全协议，例如WS-Security, WS-Policy, WS-SecureConversation, WS-ReliableMessaging...
它们提供SOAP消息头及消息体加密、数字签名等机制保障SOAP服务安全。

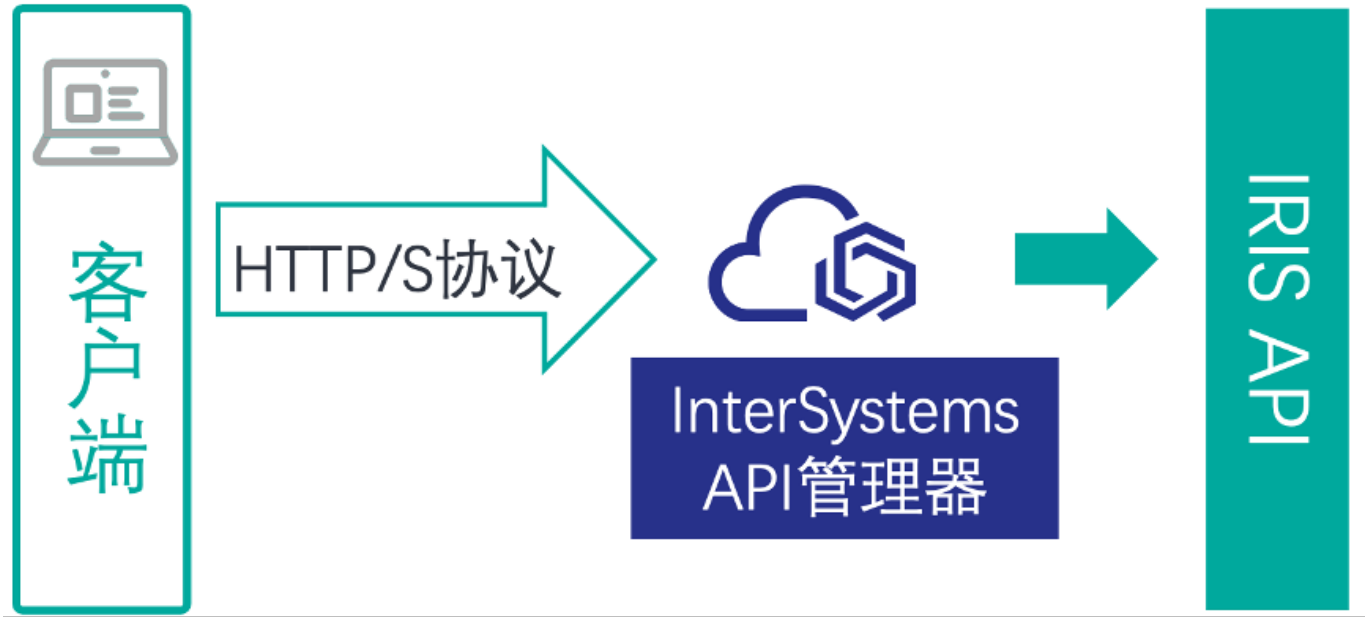
InterSystems数据平台支持这些SOAP安全协议，可以通过这些协议加强SOAP服务的安全。

8.2.4 RESTful API

RESTful
API越来越多的用于轻量化的服务提供。与SOAP服务类似，InterSystems数据平台的RESTful API也是通过Web应用提供的。

因此上面介绍的Web服务的安全检查项也适用于RESTful API应用。

另外，如果部署了InterSystems API管理器，它本身也提供了安全相关的功能，例如用户认证、权限控制等。因此也要检查InterSystems API管理器的安全设置。



8.3 安全建议

1. 不要拼接SQL语句，而是通过传参数构建运行时的SQL
2. 避免使用动态SQL
3. 启用行级安全
4. 将$ZF调用封装在方法中，避免将操作系统命令通过字符串传入
5. 部署独立的Web服务器，并启用HTTPS
6. 禁用"未验证"的身份验证方式

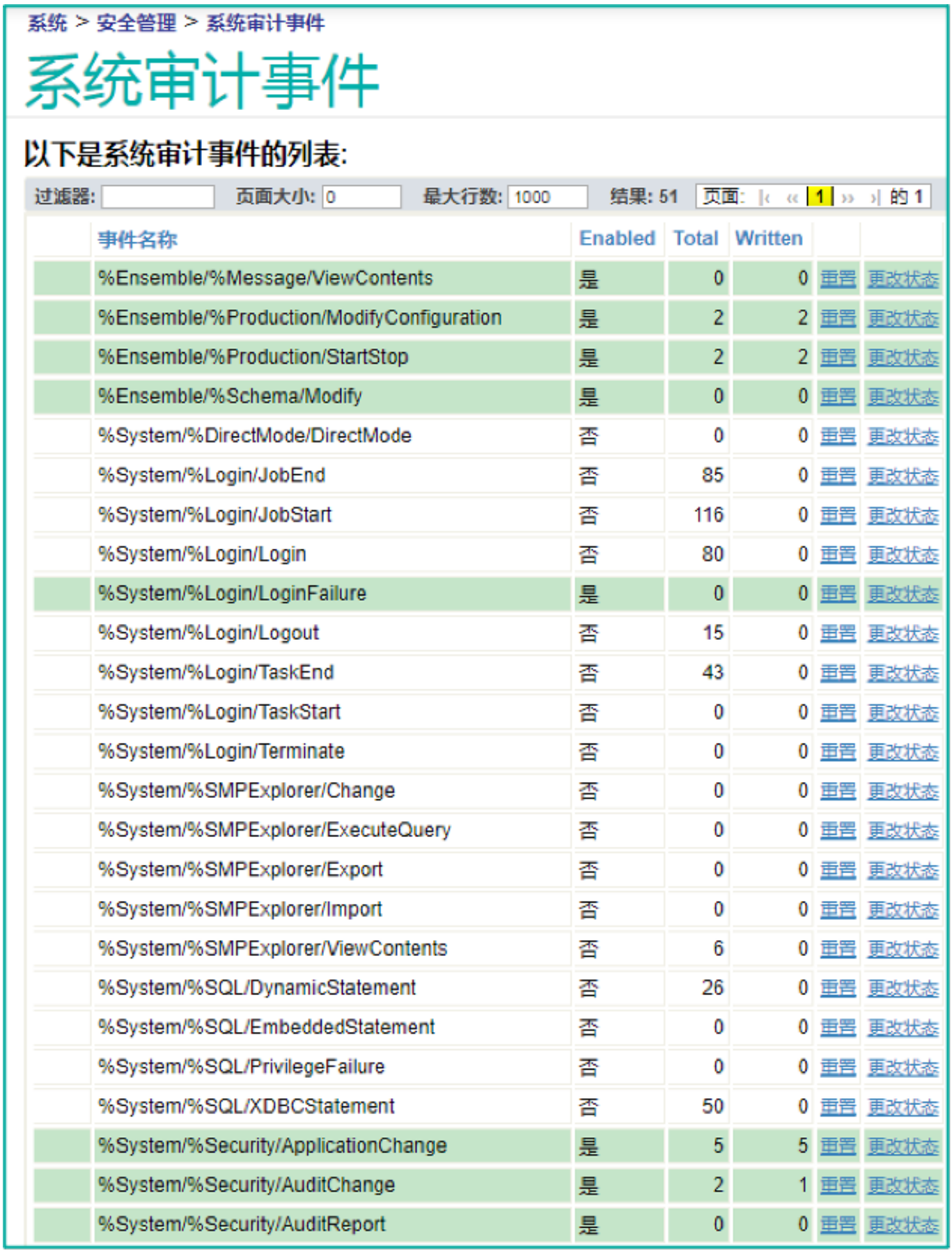
7. 选择"密码"或"Kerberos"
8. 开启防跨站请求伪造(CSRF) 攻击
9. 增加必要的资源权限要求
10. 对"应用程序角色"配置合适的角色
11. 为SOAP服务建立独立的Web应用，不使用命名空间默认的Web应用发布SOAP服务
12. 不应该发布不需要用户认证的SOAP服务和RESTful API！
13. 使用合适的认证策略，例如密码或用户名令牌
14. 使用合适的SOAP安全协议，例如消息加密、数字签名
15. 在部署了InterSystems API管理器时，通过它进一步约束安全选项

9. 安全审计

InterSystems 数据平台提供审计能力，提供防篡改的审计数据库，用于记录审计事件。审计数据可以查看、搜索和导出。

通过 ***管理门户 > 系统 > 安全管理 > 审计*** 可以开启和配置审计。

InterSystems 数据平台预置了一系列系统审计事件，例如用户登录事件、登录失败事件等。并非所有的预置系统审计都默认开启，用户可以在系统审计事件配置页面进行配置，决定审计哪些系统事件。



系统 > 安全管理 > 系统审计事件

系统审计事件

以下是系统审计事件的列表:

过滤器: 页面大小: 0 最大行数: 1000 结果: 51 页面: 1 的 1

事件名称	Enabled	Total	Written		
%Ensemble/%Message/ViewContents	是	0	0	重置	更改状态
%Ensemble/%Production/ModifyConfiguration	是	2	2	重置	更改状态
%Ensemble/%Production/StartStop	是	2	2	重置	更改状态
%Ensemble/%Schema/Modify	是	0	0	重置	更改状态
%System/%DirectMode/DirectMode	否	0	0	重置	更改状态
%System/%Login/JobEnd	否	85	0	重置	更改状态
%System/%Login/JobStart	否	116	0	重置	更改状态
%System/%Login/Login	否	80	0	重置	更改状态
%System/%Login/LoginFailure	是	0	0	重置	更改状态
%System/%Login/Logout	否	15	0	重置	更改状态
%System/%Login/TaskEnd	否	43	0	重置	更改状态
%System/%Login/TaskStart	否	0	0	重置	更改状态
%System/%Login/Terminate	否	0	0	重置	更改状态
%System/%SMPExplorer/Change	否	0	0	重置	更改状态
%System/%SMPExplorer/ExecuteQuery	否	0	0	重置	更改状态
%System/%SMPExplorer/Export	否	0	0	重置	更改状态
%System/%SMPExplorer/Import	否	0	0	重置	更改状态
%System/%SMPExplorer/ViewContents	否	6	0	重置	更改状态
%System/%SQL/DynamicStatement	否	26	0	重置	更改状态
%System/%SQL/EmbeddedStatement	否	0	0	重置	更改状态
%System/%SQL/PrivilegeFailure	否	0	0	重置	更改状态
%System/%SQL/XDBCStatement	否	50	0	重置	更改状态
%System/%Security/ApplicationChange	是	5	5	重置	更改状态
%System/%Security/AuditChange	是	2	1	重置	更改状态
%System/%Security/AuditReport	是	0	0	重置	更改状态

除了系统预置的审计事件，InterSystems数据平台运行用户自定义审计事件，例如谁修改了特定的类。通过***管理门户 >*** 系***统 > 安全管理 > 用户定义的审计事件*** 可以创建自定义审计。

9.1 安全建议

1. 开启审计
2. 对重要的用户级事件建立自定义审计事件
3. 定期分析审计的用户行为模型，识别发现异常请求

10. 备份与恢复

数据平台的备份与恢复是保障数据安全的另一项机制。定期的备份保障在意外发生时数据可以最大限度的恢复。例如是误删除了数据和代码，InterSystems数据平台的镜像高可用也无法恢复这些误删除的内容，因为误删除也会在备机上重做。这时，备份是唯一可以恢复误删除数据的希望。

所以应该有备份恢复的自动化策略，定期地执行备份，并将备份保存在与生产环境隔离的地点妥善保存。

InterSystems数据平台支持多种备份工具和备份策略。

备份工具：

冷备份 – 卸载数据库，拷贝数据库文件，加载数据库。冷备份需要计划宕机时间

联机热备份 –
InterSystems数据平台提供的在线备份，无需计划宕机时间。数据规模很大时，备份时间较长

外部备份(快照备份) – 在线备份，无需计划宕机时间。通常速度很快，但需要外部备份工具

InterSystems数据平台使用内建的联机热备份工具时，支持这些备份策略：

全备份 – 备份全部数据

增量备份 – 备份上次备份之后修改的所有数据

补充备份 - 备份上次全备份之后修改的所有数据

可以使用这些备份方式，组合成一个自动的备份计划，例如：周日执行全备份、周一周二执行增量备份、周三执行补充备份、周四周五周六执行增量备份。

这些备份文件和备份之后的所有日志文件（Journal文件）和数据平台配置文件，以及项目相关的静态文件一起，例如网页文件，才是完整的生产环境备份集。完整的备份集才能保证恢复到指定的时间节点上。

有了备份并不是万无一失，需要验证备份是否可用。应该建立备份集恢复测试的环境，定期对备份集进行恢复测试，以确保备份集是可用的。

10.1 安全建议

1. 建立自动的备份任务
    a. 备份应保存在独立的存储和隔离的物理位置
2. 定期检查备份集的可用性

11. 正确安装InterSystems数据平台

在InterSystems数据平台安装时，会提示选择安全级别。因此在安装时，就应该选择正确的安全级别，避免后期大量的安全配置检查和调整。

InterSystems数据平台安装时会提供3个安全级别选择：Minimal、Normal和Locked Down。

Minimal
：是针对于本机开发环境安装的安全级别、也是最低的安全级别，通常是被用于开发者在自己的笔记本电脑上安装InterSystems数据平台的开发实例。它几乎没有安全限制，例如允许无认证登录、匿名用户拥有%All的权限。因此绝不应该在生产环境上以此级别安装。如果您已经以Minimal安全级别安装了生产环境，那应该立刻修改安全配置。

Normal
：是针对通常用途的安全级别，收紧了安全策略，可以作为大多数生产环境的初始安全配置。建议生产环境安装时，以此级别进行安装，并在安装之后按需调整安全配置。

Locked Down
：是针对高安全需求的生产环境的安全级别。它禁用了多数服务、收紧了服务策略，因此安装后就已经提供了一个较为安全的实例。

		Minimal	Normal
安全设置	密码模式	3.32ANP	3.32AN
	不活动禁用天数*	0	90天
	启用SYSTEM用户	是	是
	分配给用户UnknownUser的角色	%All	无
服务策略	Use 权限为公共权限	是	是
	需要认证	否	是
服务	%ServiceBindings	启用	启用
	%ServiceCacheDirect	启用	禁用
	%ServiceCallIn	启用	禁用
	%ServiceComPort	禁用	禁用
	%ServiceConsole*	启用	启用
	%ServiceECP	禁用	禁用
	%ServiceMonitor	禁用	禁用
	%ServiceTelnet*	禁用	禁用
	%ServiceTerminal †	启用	启用
	%ServiceWebGateway	启用	启用

12. InterSystems 数据平台的安全建议工具

InterSystems数据平台提供安全检查和建议工具。通过***管理门户 >系统 > 安全管理 > 安全顾问***即可使用该工具。

安全建议工具会提示安全建议，点击“***详细信息***”链接，会自动跳到对应安全配置页面。在生产环境上线前，建议使用该工具进行检查。

13. InterSystems 数据平台三级等保检查清单

针对三级等保合规，检查清单如下：

- **1. 配置基于TLS的数据加密通道****
  - 所有对InterSystems 数据平台的连接方式都配置使用加密通道
- **2. 部署独立的Web服务器**
  - 配置Web服务器应用HTTPS，并禁用不安全的 HTTP 方法
- **3. 服务配置**
  - 关闭不必要的服务
  - 对必要开启的服务，选择安全的认证方式
    - 禁用“ 未验证 ”方式
  - 进一步限定允许接入的IP地址
- **4. 加强认证**
  - 系统级禁用 “ 无认证 ”
  - 选用更安全的认证方式
- **5. 收紧授权****
  - 数据库应该设置自己独立的资源，而非使用%DB%DEFAULT
  - 谨慎使用公共权限

    - 创建自己需要保护的新资源**

- **6. 用户与角色**
    - 仅管理员有%All角色
    - 要求用户账号更安全的密码模式
    - 设置密码错误数次后停用账号
- **7. 数据安全**
    - 对敏感数据进行全数据库加密
    - 合理的数据读写权限
    - 必要时，添加行级和列级安全**
- **8. 应用安全**
    - 不要拼接SQL语句，而是通过传参数构建运行时的SQL**
    - 避免使用动态SQL**
    - 启用行级安全**
    - 将$ZF调用封装在方法中，避免将操作系统命令通过字符串传入**
    - 禁用不必要的Web应用 **
    - 对Web应用，禁用"未验证"的身份验证方式
    - 对Web应用，开启防跨站请求伪造(CSRF) 攻击
    - 对Web应用，对"应用程序角色"配置合适的角色，不应随意赋予%All **
    - 为SOAP服务建立独立的Web应用，不使用命名空间默认的Web应用发布SOAP服务**
    - 不应该发布不需要用户认证的SOAP服务和REST API！
    - 使用合适的SOAP安全策略，例如消息加密、数字签名

- **9. 审计**
    - 开启审计
    - 对重要的用户级事件建立自定义审计事件 **
    - 定期分析审计的用户行为模型，识别发现异常请求 **
- **10. 备份与恢复**
    - 建立自动的备份任务
        - 备份应保存在独立的存储和隔离的物理位置
    - 定期检查备份集的可用性

注：**项目不是三级等保的必查项，但建议进行检查和配置。

#安全 #Caché #Ensemble #HealthShare #InterSystems IRIS #InterSystems IRIS for Health

---

源URL: https://cn.community.intersystems.com/post/intersystems-%E6%95%B0%E6%8D%AE%E5%B9%B3%E5%8F%B0%E4%B8%8E%E4%B8%89%E7%BA%A7%E7%AD%89%E4%BF%9D-%E7%AC%AC%E4%B8%89%E7%AF%87